IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN
GREEN BAY DIVISION

JUDITH LEITERMANN, *individually and on behalf of all others similarly situated*,

Plaintiff,

v.

FOREFRONT DERMATOLOGY, S.C. and FOREFRONT MANAGEMENT, LLC,

Defendants.

Case No. _____

CLASS ACTION COMPLAINT and JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff JUDITH LEITERMANN ("Plaintiff"), individually and on behalf of all others similarly situated, bring this class action lawsuit against FOREFRONT DERMATOLOGY, S.C., a Wisconsin service corporation, and FOREFRONT MANAGEMENT, LLC, a Delaware Limited Liability Company (collectively, "Forefront" or "Defendants") to obtain damages, restitution and injunctive relief for the Class, as defined below. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel and certain facts that are a matter of public record:

NATURE OF THE ACTION

1. This class action lawsuit arises out of the recently announced targeted ransomware cyberattack and data breach (the "Data Breach") that occurred at Forefront, a dermatology group practice comprised of more than 195 board-certified dermatologists practicing in over 175 locations in 21 states.

2. As a result of the Data Breach, Plaintiff and approximately 2,413,552 current and former patients and employees of Forefront suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or to mitigate the effects of the attack.

3. Through its public statements, Forefront appears to be attempting to minimize the breadth and severity of the Data Breach, not to mention its own negligence in allowing the breach to happen in the first place.

4. For instance, although Forefront reported the Data Breach to the Maine Attorney's General's Office as affecting "only" 4,431 persons,[1] Defendants reported the Data Breach to the United States' Department of Health and Human Service's Office for Civil Rights as affecting 2,413,553 persons.[2]

5. Moreover, in its "Notice of Data Security Incident" (the "Notice") posted on its website, Forefront describes the incident as an "intrusion into its IT network by unauthorized parties and determined that the incident resulted in unauthorized access to certain files on its IT systems that contain Forefront patient information."[3]

6. Forefront neglects to mention that the intrusion was possible (and certainly foreseeable) because of its inexcusably lax data security protocols, including incredibly simplistic passwords.

---

[1] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/f3f9c506-728b-4271-9497-95ce115e2fd0.shtml (last visited July 21, 2021).

[2] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited July 21, 2021); *see also* https://www.databreaches.net/forefront-dermatology-notifying-patients-and-employees-about-ransomware-incident/ (last visited July 21, 2021).

[3] https://forefrontdermatology.com/incidentnotice/ (last visited July 21, 2021).

7. According to an article published on www.databreaches.net on July 9, 2021 entitled *Forefront Dermatology notifying patients and employees about ransomware incident*, "[a] passwords file in the dump listed more than 100 sets of logins. **Sadly, there was what appeared to be a lot of weak password and extensive password reuse. More than 40 passwords had "Forefront" in combination with some digit(s) and an exclamation point. Another 10 had some variant of DAWderm1!**").[4]

8. As a result of Defendants' actions and inactions, Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendants—was exposed, compromised and unlawfully accessed.

9. Although the list is likely non-exhaustive, Forefront has acknowledged that the information compromised in the Data Breach includes patient names, addresses, dates of birth, patient account numbers, health insurance plan member ID numbers, medical record numbers, dates of service, accession numbers, provider names, and/or medical and clinical treatment information, and other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and additional personally identifiable information ("PII") and protected health information ("PHI") that Defendants collected and maintained (collectively, the "Private Information").

10. While Forefront boldly proclaims in the Notice posted on its website that "there is no evidence that patient Social Security numbers, driver's license numbers, or financial account/payment card information were involved in this incident," that representation is flatly contradicted by its own statements to the Maine Attorney General:

---

[4] https://www.databreaches.net/forefront-dermatology-notifying-patients-and-employees-about-ransomware-incident/ (emphasis added) (last visited July 21, 2021).

Information Acquired - Name or other personal identifier in combination with: **Social Security Number**[5]

11. Moreover, the Notice of Data Breach that Forefront submitted to the California Attorney General's Office states that it "could not rule out the possibility that files containing some of your information, including your name and Social Security number, may have been subject to unauthorized access as a result of this incident."[6]

12. Accordingly, Plaintiff brings this class action lawsuit to address Forefront's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide adequate notice to Plaintiff and Class Members that their information had been subject to unauthorized access by a third party (threat actors calling themselves Cuba Ransomware) and precisely what specific type of information was accessed.

13. Defendants maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendants' computer network in a condition vulnerable to cyberattacks, such as the one that occurred in late May to early June of this year thereby enabling access to Defendants' network and, ultimately, to the Private Information.

14. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendants, and thus it was on notice that failing to take appropriate steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

15. In addition, Defendants and its employees failed to properly monitor the computer

---

[5] https://apps.web.maine.gov/online/aeviewer/ME/40/f3f9c506-728b-4271-9497-95ce115e2fd0.shtml (last visited July 21, 2021).

[6] https://oag.ca.gov/system/files/FFM%20FFD%20-%20California%20Notification.pdf (last visited July 21, 2021).

network and systems that housed the Private Information; had Defendants properly monitored its property, it would have been able to prevent or, at least, to discover the intrusion sooner.

16. Plaintiff's and Class Members' identities are now at risk because of Defendants' negligent conduct since the Private Information that Defendants collected and maintained is now in the hands of data thieves.

17. Again, according to the Databreaches.net article, "Forefront's release does not mention any specific ransom demand or whether they negotiated at all with the threat actors. ***As of today, however, some of Forefront Dermatology's files remain freely available on the Cuba Ransomware leak site.***"[7]

18. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph and/or giving false information to police during an arrest.

19. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring

[7] https://www.databreaches.net/forefront-dermatology-notifying-patients-and-employees-about-ransomware-incident/ (emphasis added).

services, credit freezes, credit reports or other protective measures to deter and to detect identity theft.

20. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs and injunctive relief including improvements to Forefront's data security systems, future annual audits and adequate credit monitoring services funded by Defendants.[8]

PARTIES

21. Plaintiff JUDITH LEITERMANN is, and at all times mentioned herein was, an individual citizen of the State of Wisconsin residing in the City of Neenah, Wisconsin. Plaintiff was notified of Defendants' Data Breach and her Private Information being compromised upon receiving a letter titled "Notice of a Data Breach" dated as of July 8, 2021.

22. Forefront Dermatology, S.C., a Wisconsin service corporation, is a dermatology group practice comprised of more than 195 affiliated board-certified dermatologists practicing in over 175 locations in 21 states.[9]

23. Forefront Management, LLC is a Delaware Limited Liability Company registered to do business in Wisconsin.

24. Defendants maintain their corporate offices at 801 York Street in Manitowoc,

[8] While not mentioned on the Notice on its website, Forefront is evidently making a complimentary 12 month membership to TransUnion's *my*TrueIdentity Credit Monitoring Service available to affected individuals. *See* *https://oag.ca.gov/system/files/FFM%20FFD%20-%20California%20Notification.pdf*. For the reasons set forth herein, such an offer is wholly inadequate under the circumstances and in no way obviates the need for this Court to fashion appropriate and meaningful injunctive relief on behalf of the millions of impacted individuals.

[9] *See* https://forefrontdermatology.com/ (last visited July 21, 2021).

Wisconsin 54220.

25. Defendants can be served through their registered agent, CT Corporation System, 301 S. Bedford Street, Suite 1 in Madison, Wisconsin 53703.

JURISDICTION AND VENUE

26. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, Pub. L. No. 109-2 Stat. 4 ("CAFA"), which, *inter alia*, amends 28 U.S.C. § 1332, at new subsection (d), conferring federal jurisdiction over class actions where, as here: (a) there are 100 or more members in the proposed class; (b) some members of the proposed Class have a different citizenship from Defendants and (c) the claims of the proposed class members exceed the sum or value of five million dollars ($5,000,000) in aggregate. *See* 28 U.S.C. § 1332(d)(2) & (6).

27. This Court has personal jurisdiction over Defendants because (i) Forefront Dermatology, S.C. is a Wisconsin service corporation with its principal place of business in Manitowoc, Wisconsin and Forefront Management, LLC is a Delaware Limited Liability Company registered to do business in Wisconsin with its principal place of business in Manitowoc, Wisconsin, (ii) they committed tortious acts in Wisconsin and (iii) they have sufficient minimum contacts and have engaged in significant business activity in the State of Wisconsin.

28. Venue is proper in this judicial district pursuant to 18 U.S.C. §§ 1965(a) and (b) because Defendants have their principal place of business in Manitowoc, Wisconsin, regularly transact business within the geographic boundaries of this District and because the facts and circumstances giving rise to the claims asserted herein occurred within this District.

COMMON FACTUAL ALLEGATIONS

A. Forefront's Representations Regarding the Privacy and Security of its Patients' and Employees' Confidential and Protected Information.

29. Forefront Dermatology, S.C., a Wisconsin service corporation, is a dermatology group practice comprised of more than 195 board-certified dermatologists practicing in over 175 locations in 21 states.[10]

30. In the ordinary course of receiving treatment and health care services from Forefront, patients are required to provide sensitive personal and private information such as:

- Names;
- Dates of birth;
- Social Security numbers;
- Financial account information;
- Payment card information;
- Medical histories;
- Treatment information;
- Medication or prescription information;
- Provider information;
- Address, phone number and email address and
- Health insurance information.

31. Additionally, Forefront may obtain private and personal information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, patients' other doctors, patient's health plan(s), close friends and/or family members, not to mention the tremendous amount of (current and former) employee information that it possesses.

32. Due to the highly sensitive and personal nature of the information it acquires and stores with respect to its patients, Forefront makes a "Notice of Privacy Practices" available to all patients via its website.

[10] *See* https://forefrontdermatology.com/ (last visited July 21, 2021).

33. By that notice, Forefront acknowledges that "[i]t is your right as a patient to be informed of Forefront Dermatology's legal duties with respect to protection of the privacy of your protected health information ('PHI')."[11]

34. Moreover, Forefront, in its privacy policy, states

> Forefront Dermatology and its affiliates [] respect your privacy and are committed to protecting it through our compliance with this policy.

35. Finally, in its Notice of Data Breach, Forefront states that it "is committed to protecting the confidentiality and security of our current and former employees' information."[12]

36. Thus, as stated in its Notice of Privacy Practices, in its Privacy Policy and in its Notice of Data Breach, Forefront promises to maintain the confidentiality of patients' health, financial and non-public personal information, ensure compliance with federal and state laws and regulations and to notify patients of any breach that jeopardizes their private information.

37. Specifically, in a section titled "Data Security," Forefront states:

> We implement a variety of security measures for the Website to maintain the safety of your personal information from any loss, misuse or change of information that is under our control. ***Such security measures include firewalls, access restrictions and password protection.***
>
> We offer the use of a secure server. All supplied sensitive/credit information is transmitted via Secure Sockets Layer (SSL) technology and then encrypted into our payment gateway provider's database only to be accessible by those authorized with special access rights to such systems, and are required to keep the information confidential. After a transaction, your credit card information will not be stored on our servers. All other information collected through the Website will be retained for the length of time permitted by law. Personal identifiable information can be removed

[11] https://forefrontdermatology.com/wp-content/uploads/2021/05/Forefront-Dermatology-Affiliated-Practices-NOPP-1.pdf (effective as of April 23, 2021 & last visited July 21, 2021).

[12] https://oag.ca.gov/system/files/FFM%20FFD%20-%20California%20Notification.pdf.

> from our database at your request however we will retain non-personal identifiable information indefinitely.[13]

38. As a condition of receiving medical care and treatment at one of Defendants' facilities, Forefront requires that its patients entrust it with highly sensitive personal information.

39. By obtaining, collecting, using and deriving a benefit from Plaintiff' and Class Members' Private Information, Forefront assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff' and Class Members' Private Information from unauthorized access and/or disclosure.

40. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

41. Plaintiff and the Class Members relied on Forefront to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only and to make only authorized disclosures of this information.

B. Threat Actors Are Able to Access and to Make Confidential Health and Other Protected Information Publicly Available Due to Forefront's Incredibly Lax Data Security Practices.

42. According to its Notice of Data Security Incident, on June 24, 2021, Forefront Dermatology, S.C. and its affiliated practices concluded its investigation of an intrusion into its IT network by unauthorized parties and determined that the incident resulted in unauthorized access to certain files on its IT systems that contain patient information.

43. Subsequent investigation revealed that there had been unauthorized access to patient files and employee files between the dates of May 28, 2021 and June 4, 2021.

44. The patient files that were accessed may have included patient names, addresses,

[13] https://forefrontdermatology.com/privacy-policy/ (emphasis added) (last visited July 21, 2021).

dates of birth, patient account numbers, health insurance plan member ID numbers, medical record numbers, dates of service, accession numbers, provider names, and/or medical and clinical treatment information.

45. Forefront's Notice does not mention any specific ransom demand or whether they negotiated at all with the threat actors.

46. As of today, however, some of Forefront Dermatology's files remain freely available on the Cuba Ransomware leak site.[14]

47. Although not revealed in their disclosure, the attack was the work of threat actors calling themselves "Cuba Ransomware."

48. The threat actors dumped some of Forefront's data, including some patient information, at the end of the June. Also included in that dump "was more than 130 files with information on [Forefront's] system and network, with security and backup details, and all their logins to health insurance portals, etc."[15]

49. A passwords file in the dump listed more than 100 sets of logins:

> Sadly, there was what appeared to be a lot of weak password and extensive password reuse. More than 40 passwords had "Forefront" in combination with some digit(s) and an exclamation point. Another 10 had some variant of DAWderm1![16]

50. Passwords and email addresses with security questions used for one insurer's portal revealed significant re-use:

---

[14] https://www.databreaches.net/forefront-dermatology-notifying-patients-and-employees-about-ransomware-incident/

[15] *Id.*

[16] *Id.*

User	User Name	Password	Security Questions	Email address
[redacted]	[redacted]	dawderm3	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	[redacted]
		dawderm1	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	
		600York	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	
		Dawderm1	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	
		forefront4!	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	
		dawderm1	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	
		Forefront1!	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	

51. As acknowledged by Forefront, this information may have included patient names, addresses, dates of birth, patient account numbers, health insurance plan member ID numbers, medical record numbers, dates of service, accession numbers, provider names, and/or medical and clinical treatment information.[17]

52. And, as ***not*** publicly acknowledged by Forefront, the compromised information may have included Social Security numbers as well.[18]

53. While only a modest amount of the stolen information has been dumped on the Internet to date, the threat actors appear to have exfiltrated a large amount of data (meaning additional dumps of Plaintiff' and the Class Members' confidential and other private information is certainly possible).

54. Upon information and belief, the cyberattack was targeted at Forefront, due to its

[17] https://forefrontdermatology.com/incidentnotice/.

[18] https://oag.ca.gov/system/files/FFM%20FFD%20-%20California%20Notification.pdf.

status as a healthcare entity that collects, creates and maintains both PII and PHI.

55. Upon information and belief, the targeted cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII and PHI of patients and employees like Plaintiff and the Class Members.

56. Because of this cyberattack, data thieves were able to gain access to and exfiltrate the protected Private Information of hundreds of millions of Forefront patients and (current and former) employees.

57. Plaintiff's Private Information was accessed and stolen in the Data Breach.

58. Specifically, Plaintiff received a Notice from Forefront, dated as of July 8, 2021, which stated that an "intrusion result[ing] in unauthorized parties gaining access to our IT network occurred] between the dates of May 28, 2021 and June 4, 2021."[19]

59. The Notice received by Plaintiff went on to note that Forefront "could not rule out the possibility that files containing some of [its] patient information may have been subject to unauthorized access as a result of this incident."[20]

60. The information that Forefront admitted was potentially compromised includes information that it collects and maintains regarding Plaintiff and the Class Members, including, but not necessarily limited to, "name in combination with your address, date of birth, patient account number, health insurance plan member ID number, medical record number, dates of service, provider names and/or medical care and clinical treatment information."[21]

61. Plaintiff further believe their stolen Private Information was subsequently sold on

---

[19] A true and correct copy of the Notice letter received by Plaintiff is attached as **Exhibit A** hereto.

[20] See Notice, Ex. A.

[21] *Id.*

the Dark Web.

62. Further, though Forefront impliedly acknowledges that its system was inadequate to prevent such a cyberattack (and thereby protect the confidential Private Information it swore to protect), it is only offering a complimentary twelve month membership of identity monitoring services for victims.[22]

63. The offer of identity monitoring services is an acknowledgment by Forefront that the impacted customers are subject to an imminent threat of fraud and identity theft.

64. Forefront had obligations created by HIPAA, contract, industry standards, common law as well as its own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

65. Plaintiff and Class Members provided their Private Information to Forefront with the reasonable expectation and mutual understanding that it would comply with its obligations to keep such information confidential and secure from unauthorized access.

66. Forefront's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

67. In light of recent high profile data breaches at other healthcare partner and provider companies, including, American Medical Collection Agency (25 million patients, March 2019) University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), BJC

[22] *See id.*

Health System (286,876 patients, March 2020), Forefront knew or should have known that its electronic records would be targeted by cybercriminals.

68. In fact, in 2021 alone there have been over 220 data breach incidents.[23] These approximately 220 data breach incidents have impacted nearly 15 million individuals.[24]

69. Indeed, cyberattacks have become so prevalent that the Federal Bureau of Investigation and the United States Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

70. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[25]

71. According to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[26]

72. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in the medical and healthcare industries, including Defendants.

---

[23] *See* Kim Delmonico, Another (!) Orthopedic Practice Reports Data Breach, Orthopedics This Week (May 24, 2021), https://ryortho.com/breaking/another-orthopedic-practice-reports-data-breach/ (last visited July 6, 2021).

[24] *Id*.

[25] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited July 6, 2021).

[26] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited July 6, 2021).

C. Defendants Fails to Comply with FTC Guidelines.

73. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

74. According to the FTC, the need for data security should be factored into all business decision-making.

75. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities and implement policies to correct any security problems.[27]

76. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.[28]

77. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network and verify that third-party service providers have implemented reasonable security measures.

---

[27] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 6, 2021).

[28] *Id*.

78. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

79. These FTC enforcement actions include actions against healthcare providers like Defendants. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

80. Defendants failed to properly implement basic data security practices.

81. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

82. Defendants was at all times fully aware of its obligation to protect the PII and PHI of its patients.[29]

83. Defendants was also aware of the significant repercussions that would result from its failure to do so.

[29] *See* https://www.Forefronteyeclinic.com/privacy-policy ("We are required by law to maintain the privacy of protected health information and to give you this Notice explaining our privacy practices with regard to that information.").

D. Defendants Fail to Comply with Industry Standards

84. As noted above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

85. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendants, including, but not limited to, educating all employees; **strong passwords**; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data.

86. A number of industry and national best practices have been published and should be used as a go-to resource when developing an institution's cybersecurity standards.

87. The Center for Internet Security (CIS) released its *Critical Security Controls*, and all healthcare institutions are strongly advised to follow these actions. The CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[30]

88. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

[30] *See CIS Benchmarks FAQ*, Center for Internet Security, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last visited July 6, 2021).

89. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

90. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and in the healthcare administrative services industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

E. Forefront's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

91. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

92. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical and administrative components.

93. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*.

94. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Forefront left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. §

164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

95. Ransomware attacks are also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI."[31]

96. Forefront's Data Breach resulted from a combination of insufficiencies that demonstrate they failed to comply with safeguards mandated by HIPAA regulations.

F. Defendants' Conduct Breached its Obligations to its Patients and Employees.

97. Forefront breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data.

98. Forefront's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches, ransomware and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

[31] *See* 45 C.F.R. 164.40.

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

j. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

m. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process

to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

n. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act and

o. Failing to adhere to industry standards for cybersecurity.

99. As the result of, among other things, maintaining computer systems in dire need of security upgrading, *see* Notice of Data Incident, Forefront negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

100. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

101. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Forefront.

G. Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

102. Cyberattacks and data breaches at healthcare providers like Forefront are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

103. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[32]

[32] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf (last visited July 6, 2021).

104. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it.

105. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and to harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or otherwise harass or track the victim.

106. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

107. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit and correcting their credit reports.[33]

108. Identity thieves use stolen personal information such as Social Security numbers

[33] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited July 6, 2021).

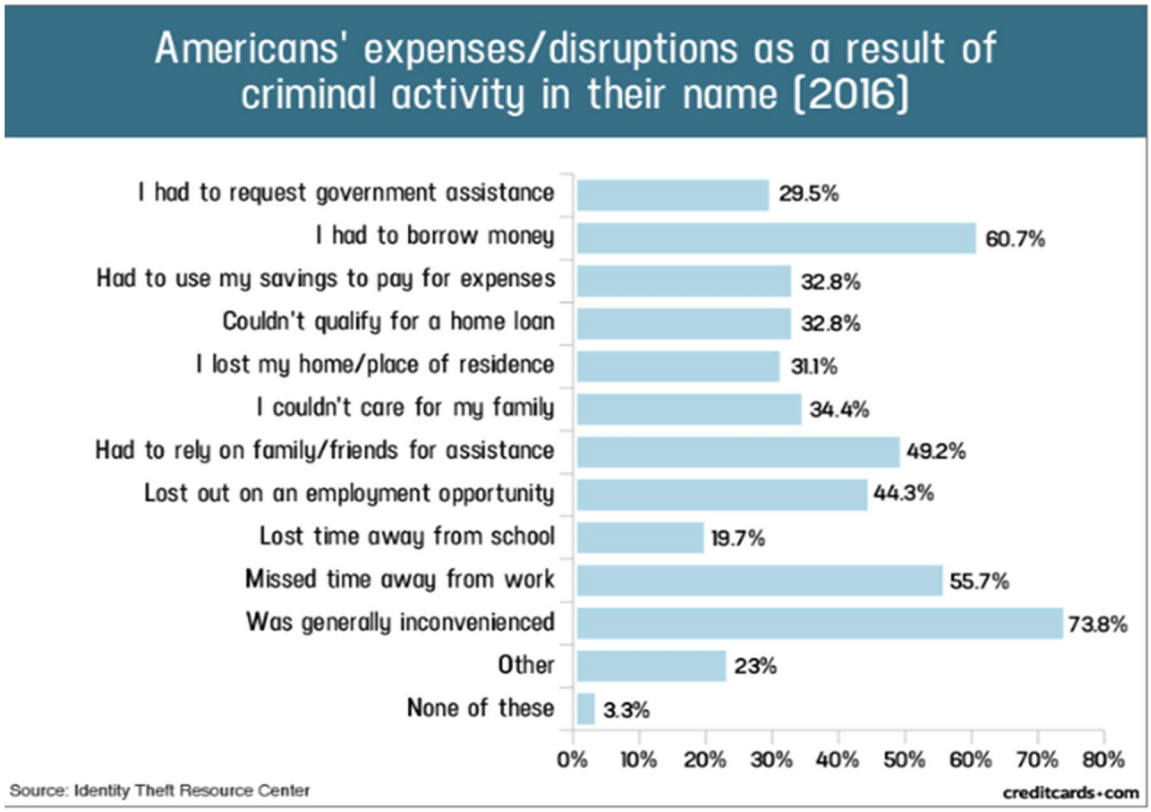
for a variety of crimes, including credit card fraud, phone or utilities fraud and bank/finance fraud.

109. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

110. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

111. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[34]

[34] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.



112. Moreover, theft of Private Information is also gravely serious; perhaps needless to say, but PII and PHI is an extremely valuable property right.[35]

113. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

114. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance

[35] *See, e.g.*, John T. Soma, *et al*., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[36]

115. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

116. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

117. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at 29.

118. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

119. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and

[36] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited July 6, 2021).

Class Members are at an increased risk of fraud and identity theft for many years into the future.

120. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

121. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[37] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

122. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[38] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[39]

123. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

124. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he

---

37 *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

38 *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 6, 2021).

39 *Id.* at 4.

credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[40]

125. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[41]

126. Medical information is especially valuable to identity thieves.

127. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[42] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[43]

128. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

129. For this reason, Forefront knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Forefront was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

---

[40] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[41] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[42] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/.

[43] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

H. Plaintiff's and Class Members' Damages

130. To date, Defendants have done virtually nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

131. The complimentary fraud and identity monitoring service offered by Forefront is wholly inadequate as the services are only offered for 12 months and it places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

132. Again consistent with the misleading nature of its "disclosures" regarding the Data Breach, Forefront does not mention on its Notice on its website or in the Notice letter received by Plaintiff (Ex. A) that it is making a complimentary 12 month membership to TransUnion's *my*TrueIdentity Credit Monitoring Service available to affected individuals.

133. Rather, the only publicly available information that suggests that Forefront is providing even that bare minimum is set forth in its notice to the California Attorney General.[44]

134. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

135. Plaintiff's PII and PHI was compromised as a direct and proximate result of the Data Breach.

136. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been placed at an imminent, immediate and continuing increased risk of harm from fraud and identity theft.

137. As a direct and proximate result of Defendants' conduct, Plaintiff and Class

[44] *See* https://oag.ca.gov/system/files/FFM%20FFD%20-%20California%20Notification.pdf (last visited July 21, 2021).

Members have been forced to expend time dealing with the effects of the Data Breach.

138. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud and similar identity theft.

139. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, ransomware and other illegal schemes based on their Private Information.

140. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees and similar costs directly or indirectly related to the Data Breach.

141. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach.

142. Numerous courts have recognized the propriety of loss of value damages in related cases.

143. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to Forefront was intended to be used by Defendants to fund adequate security of Forefront's computer property and to protect Plaintiff' and Class Members' Private Information.

144. In short, Plaintiff and the Class Members did not get what they paid for.

145. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

146. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket

expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges, insurance claims and/or government benefit claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with credit reporting agencies;

d. Spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims;

e. Contacting financial institutions and closing or modifying financial accounts;

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts and credit reports for unauthorized activity for years to come.

147. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants (in some form), is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected and that such data is properly encrypted.

148. Further, as a result of Forefront's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

149. As a direct and proximate result of Forefront's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at an increased risk of future harm.

CLASS REPRESENTATION ALLEGATIONS

150. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff seek certification of the following class of persons defined as follows:

> **National Class:** All persons Forefront identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.

Excluded from the Classes are any judges presiding over this matter and court personnel assigned to this case.

151. **Numerosity**: The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, the Classes reportedly include approximately 2,413,553 current and former patients and employees of Forefront. The identities of Class Members are ascertainable through Forefront's records, Class Members' records, publication notice, self-identification and other means.

152. **Commonality**. There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Forefront unlawfully used, maintained, lost or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Forefront failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Forefront's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations, *e.g.*, HIPAA;

d. Whether Forefront's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Forefront owed a duty to Class Members to safeguard their Private Information;

f. Whether Forefront breached its duty to Class Members to safeguard their Private Information;

g. Whether hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Forefront knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Forefront owed a duty to provide Plaintiff and Class Members notice of this Data Breach, and whether Defendants breached that duty to provide timely and accurate notice;

j. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Forefront's misconduct;

k. Whether Forefront's conduct was negligent;

l. Whether Forefront's conduct violated federal law;

m. Whether Forefront's conduct violated state law and

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages and/or injunctive relief.

153. Common sources of evidence may also be used to demonstrate Forefront's unlawful conduct on a class-wide basis, including, but not limited to, documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can prove

Forefront's data and cybersecurity systems have been or remain inadequate; documents and testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach.

154. **Typicality**. Plaintiff' claims are typical of the claims of the respective Class she seeks to represent, in that the named Plaintiff and all members of the proposed Class have suffered similar injuries as a result of the same practices alleged herein. Plaintiff have no interests adverse to the interests of the other members of the Class.

155. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff' Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

156. **Predominance**. Forefront has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

157. **Superiority**. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Forefront.

In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

158. Forefront has acted on grounds that apply generally to the Classes as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

159. Certification is appropriate because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Forefront owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing and safeguarding their Private Information;

b. Whether Forefront's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Forefront's failure to institute adequate protective security measures amounted to negligence;

d. Whether Forefront failed to take commercially reasonable steps to safeguard consumer Private Information and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

160. Finally, all members of the proposed Classes are readily ascertainable. Forefront has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Forefront.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Classes)

161. Plaintiff repeat and re-allege each and every factual allegation contained in paragraphs 1-160 as if fully set forth herein.

162. Plaintiff bring this claim individually and on behalf of the Class Members.

163. In order to receive medical treatments and services, Forefront and/or its Affiliates required Plaintiff and Class Members to submit non-public Private Information, such as PII and PHI.

164. Plaintiff and Class Members entrusted their Private Information to Forefront and/or its Affiliates with the understanding that Forefront would safeguard their information.

165. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Forefront and its Affiliates had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft.

166. Defendants' duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

167. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

168. Defendants' duty of care to use reasonable security measures arose as a result of

the special relationship that existed between Defendants and its client patients, which is recognized by laws and regulations including, but not limited to, HIPAA, as well as common law.

169. Defendants was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

170. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

171. Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

172. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

173. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants is bound by industry standards to protect confidential Private Information.

174. Defendants breached its duties and thus was negligent by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

d. Failing to adequately train its employees to recognize and contain phishing attacks;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

g. Failing to timely notify Class Members about the Cyber-Attack regarding what type of Private Information had been compromised so that they could take appropriate steps to mitigate the potential for identity theft and other damages and

h. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

175. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members.

176. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

177. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

178. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

179. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen its data security systems and monitoring procedures; (ii) submit to

future annual audits of those systems and monitoring procedures and (iii) continue to provide adequate credit and identity monitoring to all Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Classes)

180. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

181. Through their course of conduct, Defendants, Plaintiff and Class Members entered into implied contracts for the provision of healthcare and treatment, as well as implied contracts for Defendants to implement data security adequate to safeguard and to protect the privacy of Plaintiff' and Class Members' Private Information.

182. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendants when she first went for medical care and treatment at one of Defendants' facilities.

183. The valid and enforceable implied contracts to provide medical health care services that Plaintiff and Class Members entered into with Defendants and/or its Agents include the promise to protect non-public Private Information given to Defendants or that Defendants creates on its own from disclosure.

184. When Plaintiff and Class Members provided their Private Information to Defendants and/or its Affiliates in exchange for medical services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

185. Defendants and/or its agents solicited and invited Class Members to provide their Private Information as part of Defendants' regular business practices.

186. Plaintiff and Class Members accepted Defendants' offers and provided their Private

Information to Defendants.

187. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

188. Class Members who paid money to Defendants reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security. Defendants failed to do so.

189. Under the implied contracts, Defendants and/or its Affiliates promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members and (b) protect Plaintiff' and the Class Members' PII/PHI: (i) provided to obtain such health care and/or (ii) created as a result of providing such health care. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

190. Both the provision of medical services healthcare and the protection of Plaintiff' and Class Members' Private Information were material aspects of these implied contracts.

191. The implied contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiff' and Class Members' Private Information—are also acknowledged, memorialized and embodied in certain documents, including (among other documents) Defendants' Privacy Policy and Notice of Data Incident.

192. Defendants' express representations, including, but not limited to, the express representations found in its Privacy Policy, memorializes and embodies the implied contractual obligation requiring Defendants to implement data security adequate to safeguard and to protect the privacy of Plaintiff's and Class Members' Private Information.

193. Consumers of healthcare value their privacy, the privacy of their dependents and

the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security.

194. Plaintiff and Class Members would not have entrusted their Private Information to Defendants and/or its Affiliates and entered into these implied contracts with Defendants without an understanding that their Private Information would be safeguarded and protected or entrusted their Private Information to Defendants in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

195. A meeting of the minds occurred as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendants and/or its Agents, and paid for the provided healthcare in exchange for, amongst other things, both the provision of health care and medical services and the protection of their Private Information.

196. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

197. Defendants materially breached its contractual obligation to protect the non-public Private Information Defendants gathered when the sensitive information was accessed by unauthorized personnel as part of the Data Breach.

198. Defendants materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Privacy Policy.

199. Forefront did not maintain the privacy of Plaintiff' and Class Members' Private Information as evidenced by its notifications of the Data Breach to Plaintiff and approximately 2,413,553 Class Members.

200. Specifically, Defendants did not comply with industry standards, standards of conduct embodied in statutes like HIPAA and Section 5 of the FTCA or otherwise protect Plaintiff' and the Class Members' Private Information, as set forth above.

201. The Cyber-Attack and Data Breach was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

202. As a result of Defendants' failure to fulfill the data security protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received health care and other medical services that were of a diminished value to that described in the contracts.

203. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the health care they received.

204. Had Defendants disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members nor any reasonable person would have purchased healthcare from Defendants and/or its affiliated healthcare providers.

205. As a direct and proximate result of the Cyber-Attack/Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendants.

206. Plaintiff and Class Members are entitled to compensatory and consequential

damages suffered as a result of the Cyber-Attack/Data Breach.

207. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures and (iii) immediately provide adequate credit and identity monitoring to all Class Members.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Classes)

208. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

209. This count is plead in the alternative to the breach of contract count above.

210. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they purchased goods and services from Defendants and/or its Agents and in so doing provided Defendants with their Private Information.

211. In exchange, Plaintiff and Class Members should have received from Defendants the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

212. Defendants knew that Plaintiff and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

213. The amount Plaintiff and Class Members paid for goods and services were used, in part, to pay for use of Defendants' network and the administrative costs of data management and security.

214. Under the principles of equity and good conscience, Defendants should not be

permitted to retain the money belonging to Plaintiff and Class Members because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

215. Defendants failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

216. Defendants acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

217. If Plaintiff and Class Members knew that Defendants had not reasonably secured their Private Information, they would not have agreed to Defendants' services.

218. Plaintiff and Class Members have no adequate remedy at law.

219. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect Private Information in their continued possession and (g) future costs in terms of time, effort, and money that will be expended

to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

220. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

221. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants' services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff JUDITH LEITERMANN, individually and behalf of all others similarly situated, prays for relief as against FOREFRONT DERMATOLOGY, S.C. and FOREFRONT MANAGEMENT, LLC as follows:

A. For an Order certifying this case as a class action pursuant to Federal Rule of Civil Procedure 23, appointing Plaintiff as Class Representatives and the undersigned attorneys as Class Counsel;

B. Awarding monetary, punitive and actual damages and/or restitution, as appropriate;

C. Awarding declaratory and injunctive relief as permitted by law or equity to ensure that the Class has an effective remedy, including enjoining Forefront from continuing the unlawful practices as set forth above;

D. Prejudgment interest to the extent allowed by the law;

E. Awarding all costs, experts' fees and attorneys' fees, expenses and costs of prosecuting this action and

F. Such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury of all claims so triable.

Dated this 28th day of July 2021.

Respectfully submitted,

s/ *Joseph S. Goode*

Joseph S. Goode
John W. Halpin
LAFFEY, LEITNER & GOODE LLC
325 E. Chicago St., Suite 200
Milwaukee, WI 53202
Tel: (414) 312-7003
jgoode@llgmke.com
jhalpin@llgmke.com

Gary E. Mason*
David K. Lietz*
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW
Suite 305
Washington, DC 20016
Tel: (202) 429-2290
gmason@masonllp.com
dlietz@masonllp.com

Gary M. Klinger*
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (202) 429-2290
gklinger@masonllp.com

**pro hac vice to be filed*

Attorneys for Plaintiff & the Proposed Class